IN THE CLAIMS

1. (Currently Amended)   A method for implementing a security filter for regulating access to data associated with a reporting system, comprising the steps of:

enabling a user to submit a user identification input and a user request to a reporting system an on-line analytical processing system;

identifying the user based on user identification input;

retrieving data associated with the on-line analytical processing system in accordance with the user request;

filtering the retrieved data based on at least one security filter associated with the identified user; and

presenting the data as a report to the user through a user interface.

2. (Original)   The method of claim 1 wherein the security filter comprises a filter expression that specifies a subset of data in at least one database.

3. (Original)   The method of claim 2 wherein the security filter comprises a top range attribute that specifies a highest level of analysis to which the security filter is applied.

4. (Original)   The method of claim 2 wherein the security filter comprises a bottom range attribute that specifies a lowest level of analysis to which the security filter is applied.

5. (Original)   The method of claim 1 wherein the user is associated with a group of users wherein the security filter is a group level security filter.

6. (Original)   The method of claim 2 wherein the security filter varies by user and at least one fact/metric element.

7. (Currently Amended)   A system for implementing a security filter for regulating

access to data associated with a reporting system, comprising:

a user input for enabling a user to submit a user identification input and a user request to

~~a reporting system~~ an on-line analytical processing system;

an identification module for identifying the user based on user identification input;

an access module for retrieving data associated with the on-line analytical processing

system in accordance with the user request;

at least one security filter for filtering the retrieved data wherein the at least one security

filter is associated with the identified user; and

a user interface for presenting the data as a report to the user.

8. (Original)   The system of claim 7 wherein the security filter comprises a filter

expression that specifies a subset of data in at least one database.

9. (Original)   The system of claim 8 wherein the security filter comprises a top range

attribute that specifies a highest level of analysis to which the security filter is applied.

10. (Original)   The system of claim 8 wherein the security filter comprises a bottom range

attribute that specifies a lowest level of analysis to which the security filter is applied.

11. (Original)   The system of claim 7 wherein the user is associated with a group of users

wherein the security filter is a group level security filter.

12. (Original)   The system of claim 8 wherein the security filter varies by user and at least

one fact/metric element.

13. (Currently Amended)   A processor-readable medium comprising code for execution by a processor to implement a security filter for regulating access to data associated with a reporting system, the medium comprising:

code for causing a processor to enable a user to submit a user identification input and a user request to ~~a reporting system~~ an on-line analytical processing system;

code for causing a processor to identify the user based on user identification input;

code for causing a processor to retrieve data associated with the on-line analytical processing system in accordance with the user request;

code for causing a processor to filter the retrieved data based on at least one security filter associated with the identified user; and

code for causing a processor to present the data as a report to the user through a user interface.

14. (Original) The medium of claim 13 wherein the security filter comprises a filter expression that specifies a subset of data in at least one database.

15. (Original) The medium of claim 14 wherein the security filter comprises a top range attribute that specifies a highest level of analysis to which the security filter is applied.

16. (Original) The medium of claim 14 wherein the security filter comprises a bottom range attribute that specifies a lowest level of analysis to which the security filter is applied.

17. (Original) The medium of claim 13 wherein the user is associated with a group of users wherein the security filter is a group level security filter.

18. (Original) The medium of claim 14 wherein the security filter varies by user and at least one fact/metric element.